AMENDMENTS TO THE CLAIMS

1.   **(Currently Amended)** A medical information system comprising:

a patient server comprising a first database, said patient server being operable to receive vital information and unique identifications, store and manage the received vital information and unique identifications in said first database such that the vital information is ~~not~~ associated with a corresponding unique identification, and transmit the stored and managed vital information and unique identifications, wherein said first database does not store patient data;

a medical care provider server connected to said patient server through a first network and comprising a second database, said medical care provider server being operable to receive the vital information, and unique identifications from said first database of said patient server through the first network, store and manage the received vital information, unique identifications, and patient data in said second database, associate each of the unique identifications with corresponding patient data, identify corresponding patient data using each of the unique identifications, and allow the stored and managed vital information, unique identifications, and patient data to be browsed;

a patient terminal connected to said patient server through a second network, said patient terminal being operable to transmit the vital information and unique identifications to said patient server through the second network; and

a doctor terminal connected to said medical care provider server through a third network, said doctor terminal being operable to browse the vital information, patient identifications, and patient data stored and managed in said medical care provider server through the third network.

2.   **(Cancelled)**

3.   **(Previously Presented)** A medical information system according to claim 1, further comprising a sensor for measuring vital data, wherein the vital information includes a measurement value by said sensor.

4.	(Previously Presented) A medical information system according to claim 1, wherein:

said doctor terminal is operable to transmit, as consultation data, an inquiry regarding a health status of a patient to said medical care provider server through the third network; and

the vital information transmitted from said patient terminal to said patient server through the second network includes a reply to the inquiry transmitted to said patient terminal.

5.	(Previously Presented) A medical information system according to claim 1, further comprising:

a first unauthorized access prevention section provided in the first network;

a second unauthorized access prevention section provided in the second network; and

a third unauthorized access prevention section provided in the third network,

wherein said first and third unauthorized access prevention sections have higher security levels than a security level of said second unauthorized access prevention section.

6.	(Previously Presented) A medical information system according to claim 5, wherein:

said first unauthorized access prevention section comprises a firewall and a virtual private network;

said second unauthorized access prevention section comprises a remote access server; and

said third unauthorized access prevention section comprises a terminal authentication server.

7.	(Previously Presented) A medical information system according to claim 1, wherein said patient server and said medical care provider server are respectively clustered.

8. **(Currently Amended)** A medical information system comprising:

a plurality of patient servers each comprising a first database and each patient server being operable to receive vital information and unique identifications, store and manage the received vital information and unique identifications in a respective first database such that the vital information is ~~not~~ associated with a corresponding unique identification, and transmit the stored and managed vital information and unique identifications, wherein said first databases do not store patient data;

a medical care provider server connected to said plurality of patient servers through a first network and comprising a second database, said medical care provider server being operable to receive the vital information and unique identifications from each of said first databases of said plurality of patient servers through the first network, store and manage the received vital information, unique identifications, and patient data, associate each of the unique identifications with corresponding patient data, identify the corresponding patient data using each of the unique identifications, and allow the stored and managed vital information, unique identifications, and patient data to be browsed;

a plurality of patient terminals each connected to at least one of said patient servers through a second network, said patient terminals being operable to respectively transmit the vital information and unique identifications to said patient servers through the second network; and

a doctor terminal connected to said medical care provider server through a third network, said doctor terminal being operable to browse the vital information, unique identifications, and patient data stored and managed in said medical care provider server through the third network.

9. **(Currently Amended)** A medical information system comprising:

a patient server comprising a first database, said patient server being operable to receive vital information and unique identifications, store and manage the received vital information and said unique identifications such that the vital information is ~~not~~ associated with a corresponding unique identification, and transmit the stored and

managed vital information and unique identifications, wherein said patient server does not store patient data;

a plurality of medical care provider servers connected to said patient server through a first network and each comprising a second database, said medical care provider servers being operable to respectively receive the vital information and unique identifications from said patient server through the first network, store and manage the received vital information, unique identifications and patient data in said second database, associate each of the unique identifications with corresponding patient data, identify corresponding patient data using each of the unique identifications, and allow the stored and managed vital information, unique identifications, and patient data to be browsed;

a patient terminal connected to said patient server through a second network, said patient terminal being operable to transmit the vital information and unique identifications to said patient server through the second network; and

a plurality of doctor terminals each connected to at least one of said medical care provider servers through a third network, said plurality of doctor terminals being operable to browse the vital information, unique identifications, and patient data stored and managed in said medical care provider servers through the third network, respectively.

10.   (Previously Presented) A medical information system according to claim 8, wherein each of said plurality of patient terminals includes a sensor for measuring vital data, and the vital information includes a measurement value by said sensor.

11.   (Previously Presented) A medical information system according to claim 8, wherein:

said doctor terminal is operable to transmit, as consultation data, an inquiry regarding a health status of a patient to said medical care provider server through the third network;

the vital information transmitted from one of said patient terminals to a corresponding patient server through the second network includes a reply to the inquiry transmitted to said one of said patient terminals.

12.   (Previously Presented) A medical information system according to claim 8, further comprising:

a first unauthorized access prevention section provided in the first network;

a second unauthorized access prevention section provided in the second network; and

a third unauthorized access prevention section provided in the third network,

wherein said first and third unauthorized access prevention sections have higher security levels than a security level of said second unauthorized access prevention section.

13.   (Previously Presented) A medical information system according to claim 12, wherein:

said first unauthorized access prevention section comprises a firewall and a virtual private network;

said second unauthorized access prevention section comprises a remote access server; and

said third unauthorized access prevention section comprises a terminal authentication server.

14.   (Previously Presented) A medical information system according to claim 9, wherein said patient terminal includes a sensor for measuring vital data, and the vital information includes a measurement value by said sensor.

15.   (Previously Presented) A medical information system according to claim 9, wherein:

each of said plurality of doctor terminals is operable to transmit, as consultation data, an inquiry regarding a health status of a patient through the third network to a respective one of said plurality of medical care provider servers; and

the vital information transmitted from said patient terminal to said patient server through the second network includes a reply to the inquiry transmitted to said patient terminal.

16.   **(Previously Presented)** A medical information system according to claim 9, further comprising:

a first unauthorized access prevention section provided in the first network;

a second unauthorized access prevention section provided in the second network; and

a third unauthorized access prevention section provided in the third network,

wherein said first and third unauthorized access prevention sections have higher security levels than a security level of said second unauthorized access prevention section.

17.   **(Previously Presented)** A medical information system according to claim 16, wherein:

said first unauthorized access prevention section comprises a firewall and a virtual private network;

said second unauthorized access prevention section comprises a remote access server; and

said third unauthorized access prevention section comprises a terminal authentication server.